Claims 9, 15, 17, and 25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Son in view of Fruehauf and Pinder (US 6,105,134).

Applicants respectfully request reconsideration of these rejections in view of the following comments.

Discussion of Cited References

As discussed in a telephone conference with the Examiner on May 26, 2004, it is apparent from the Examiner's comments set forth in the Response to Arguments section of the Office Action that the Examiner has a basic misunderstanding of either the present invention as claimed or the Son reference. During this telephone discussion, the Examiner promised to telephone Applicants' undersigned counsel upon consideration of Applicants' written Response rather than consent to a substantive telephone interview regarding the final Office Action. In the event the Examiner has any questions or does not find this Response to be persuasive, the Examiner is requested to telephone Applicants' undersigned counsel as promised.

In the final Office Action, the Examiner continues to assert that Son discloses that the remote server 404 (which the Examiner equates with Applicants' claimed secondary CAP) provides the encrypted data stream and first and second CA data to a plurality of user terminals. The Examiner is mistaken in asserting that the server 404 of Son provides two types of CA data to the user terminals. The remote server 404 of Son provides only the re-encrypted program and the second key to the subscriber stations 110. In Son, the first key is used to decrypt the encrypted program at the server 404. The program is re-encrypted at the server 404 using a second key. Therefore, it is this second key that is needed by the terminals to decrypt the re-encrypted data.

Accordingly, in Son, the terminals receive the encrypted

program and only the second key (Col. 4, lines 11-23). In Son, the first key is not forwarded to the terminals. In addition, it would make no sense to forward the first key to the terminals along with the encrypted data and the second key as apparently assumed by the Examiner, because the first key would be useless at the user terminal since the program, which was originally encrypted using the first key, was decrypted at the server 404 and re-encrypted using a different second key. As only the second key is needed at the terminal in Son to decrypt the re-encrypted program, only the second key is sent to the terminals.

In contrast with Son, with Applicants' invention, the data stream provided to the terminals is comprised of the encrypted data service, as well as the conditional access (CA) data in the first format of the primary CAP and also CA data in the second format of the secondary CAP. This enables terminals which are compatible with the first CA data to decrypt the encrypted data service and user terminals which are compatible with the second CA to decrypt the same encrypted service. In other words, the present invention, by sending out one encrypted data service together with two different sets of CA data (each set having a different format), enables different terminals which require conditional access data in different formats to decrypt the encrypted data service.

Further, with Applicants' claimed invention, the encrypted data service, once encrypted using the first CA data does not change. In other words, the encrypted data service of Applicants' claims is not decrypted and re-encrypted at the secondary CAP as is the encrypted program of Son, which is decrypted and re-encrypted at the server 404 using the second key. With Applicants' claimed invention, the data service encrypted with the first CA data may be decrypted using the second CA data at a terminal compatible with the second CA data, or decrypted using the first CA data at a terminal compatible with the first CA

data.

In addition, the first and second key used by the server of Son are independent from one another. In contrast, with Applicants' claimed invention, the secondary CAP provides the second CA data in a different, second format in response to the first CA data and time data. Son does not disclose or remotely suggest that the server 404 provides the second key in response to the first key and time data. Further, the first and second keys of Son are provided in the same format, and these keys are not equivalent to first CA data in a first format and second CA data in a second, different format as claimed by Applicants.

In the embodiment described in column 5 of Son referenced by the Examiner, the server 404 does not provide second conditional access data in response to the first conditional access data, as claimed by Applicants. Instead, the server 404 of Son merely acts as a pass through for the encrypted video program and encryption key (Col. 5, lines 4-5). In other described embodiments of Son as discussed above, the server 404 may decrypt the encrypted program and re-encrypt it in a second form before transmitting it to the subscriber station 110. However, in this embodiment of Son, only the second encrypted form of the video program and the second key are sent to the subscriber station 110. The first key is not sent as it cannot be used to decrypt a program encrypted using the second key.

In contrast, with Applicants' claimed invention, a data stream comprising the at least one encrypted data service and first conditional access data and second conditional access data are provided to at least first and second user terminals, including a first user terminal that is compatible with the first conditional access data and a second user terminal that is compatible with the second conditional access data.

Son does not disclose or remotely suggest providing first and second conditional access data to user terminals where the

first and second conditional access data are in two different formats to user terminals compatible with different conditional access systems to decrypt the same encrypted data, as provided by Applicants' claimed invention.

Further, Son describes a point-to-point video-on-demand system. Therefore, the encrypted program of Son is sent to only the one particular subscriber unit that requested the program together with the particular decryption key needed to decrypt the encrypted program. In contrast, the data stream of Applicants' claimed invention is sent to at least first and second user terminals, the fist user terminal being compatible with the first CA data and the second user terminal being compatible with the second CA data. Therefore, in contrast with Son, Applicants' claimed invention is designed for use, for example, in a television broadcast environment where a plurality of different subscribers may have different types of user terminals which have different requirements (e.g., different formats) for conditional access data (Applicants' specification, page 1, lines 10-13). To enable the different types of subscriber terminals to co-exist in the same broadcast system, the present invention provides conditional access data in a first format for encrypting at least one data service during a plurality of successive crypto-periods and time data for identifying the successive crypto-periods from a primary CAP to a secondary CAP. The secondary CAP is responsive to the first conditional access data and time data and provides second conditional access data in a different, second format for the successive crypto-periods. A data stream comprising the at least one encrypted data service and the first and second conditional access data is provided to user terminals, including at least a first user terminal that is compatible with the first conditional access data and a second user terminal that is compatible with the second conditional access data.

Son is directed at providing increased security in a point-

to-point video on demand system, and does not address the problem of different types of user terminals in a broadcast system that require conditional access data in different formats, which is solved by Applicants' invention.

Simply put, with Applicants' claimed invention, the data stream that is sent to at least the first and second terminals comprises three items:

(1) the encrypted data service which was encrypted using the first CA data;

(2) the first CA data in a first format; and

(3) the second CA data in a second, different format.

In contrast, the data stream of Son, which is sent to a single terminal, comprises only two items:

(1) the re-encrypted program which was re-encrypted using the second key; and

(2) the second key (if necessary).

There is simply no disclosure or suggestion in Son that the data stream sent to the terminal includes both first CA data in a first format and second CA data in a second format, in addition to the encrypted program, as is claimed by Applicants.

Fruehauf does not cure the deficiencies of Son discussed above. Thus, the proposed combination of Son and Fruehauf does not render Applicants' claims obvious.

In view of the above, Applicants respectfully submit that the present invention would not have been obvious to one skilled in the art in view of Son in combination with Fruehauf or any of the other references of record.

In light of the foregoing, withdrawal of the rejections under 35 U.S.C. § 103(a) is respectfully requested.

Further remarks regarding the asserted relationship between Applicants' claims and the prior art are not deemed necessary, in view of the above discussion. Applicants' silence as to any of the Examiner's comments is not indicative of an acquiescence to

the stated grounds of rejection.

Conclusion

The Examiner is respectfully requested to reconsider this application, allow each of the presently pending claims, and to pass this application on to an early issue.

If there are any remaining issues that need to be addressed in order to place this application into condition for allowance, the Examiner is requested to telephone Applicants' undersigned attorney as agreed during the May 26, 2004 telephone conference.

Respectfully submitted,

Douglas M. McAllister
Attorney for Applicant(s)
Law Office of Barry R. Lipsitz
Registration No. 37,886
755 Main Street
Monroe, CT 06468
(203) 459-0200

ATTORNEY DOCKET NO.: GIC-599
Date: May 27, 2004